# Вступление

Этот документ и все другие части, связанные с ним, были разработаны в ответ на мировой спрос на устройства Интернета вещей (IoT), ориентированные на умный дом, такие как бытовая техника, дверные замки, камеры безопасности, датчики и исполнительные механизмы; они должны быть смоделированы и надежно управляться локально и удаленно через IP-сеть.

Хотя существовала некоторая связь между устройствами, универсального языка для Интернета вещей не было разработано. Вместо этого производителям устройств приходилось выбирать между разрозненными фреймворками, ограничивающими свою долю рынка, или разработкой в ​​нескольких экосистемах, увеличивая свои затраты. Затем на конечных пользователей ложится бремя: определить, совместимы ли продукты, которые они хотят, с экосистемой, в которую они купили, или найти способы интегрировать свои устройства в свою сеть и попытаться самостоятельно решить проблемы совместимости.

Помимо умного дома развертыванию Интернета вещей в коммерческих средах препятствует недостаточная безопасность. Этой проблемы можно избежать, используя безопасную структуру связи IoT, которую решает этот стандарт.

Целью этих документов является подключение следующих 25 миллиардов устройств для Интернета вещей, обеспечивая безопасное и надежное обнаружение устройств и возможность подключения между несколькими ОС и платформами. Существует множество предложений и форумов, в которых используются разные подходы, но ни одно решение не удовлетворяет большинство ключевых требований. Этот документ и связанные с ним части позволяют объединить отрасль вокруг единого, безопасного и совместимого подхода.

# 1 Scope

This document defines functional requirements for the OCF Cloud to Cloud Application

Programming Interface (API).

# 2 Normative references

OCF Cloud API for Cloud Services <https://github.com/openconnectivityfoundation/core-extensions/blob/ocfcloud-openapi/swagger2.0/oic.r.cloudopenapi.swagger.json>

OpenAPI 2.0, fka Swagger RESTful API Documentation Specification, Version 2.0

<https://github.com/OAI/OpenAPI-Specification/blob/master/versions/2.0.md>

# 3 Terms, definitions, and abbreviated terms

## 3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in [ISO/IEC 30118-1](#_bookmark11) and [ISO/IEC](#_bookmark12) [30118-2](#_bookmark12) and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

– ISO Online browsing platform: available at <https://www.iso.org/obp>

– IEC Electropedia: available at <http://www.electropedia.org/>

### 3.1.1 API Endpoint

определенный URL-адрес, на который отправляются запросы, определенные в этом документе

### 3.1.2 Bearer Token

OAuth2.0 токен доступа, как определено в [IETF RFC 6750](#_bookmark6)

### 3.1.3 Origin Cloud

OCF Cloud или стороннее облако, через которое пользователь работает со своими устройствами OCF.

### 3.1.4 Subscription ID

уникальный идентификатор, связанный с экземпляром подписки на событие (или события)

### 3.1.5 Target Cloud

OCF Cloud, к которому подключены серверы OCF (устройства OCF), которыми пользователь хочет управлять через Origin Cloud ([3.1.2](#_bookmark18))

## 3.2 Symbols and abbreviated terms

API Application Programming Interface

HMAC Hash-based Message Authentication Code

# 4 Document conventions and organization

## 4.1 Conventions

In this document a number of terms, conditions, mechanisms, sequences, parameters, events, states, or similar terms are printed with the first letter of each word in uppercase and the rest lowercase (e.g., Network Architecture). Any lowercase uses of these words have the normal technical English meaning.

In this document, to be consistent with the IETF usages for RESTful operations, the RESTful operation words CRUDN, CREATE, RETRIVE, UPDATE, DELETE, and NOTIFY will have all letters capitalized. Any lowercase uses of these words have the normal technical English meaning.

## 4.2 Notation

In this document, features are described as required, recommended, allowed or DEPRECATED as follows:

Required (or shall or mandatory)(M).

– These basic features shall be implemented to comply with Core Architecture. The phrases "shall not", and "PROHIBITED" indicate behaviour that is prohibited, i.e. that if performed means the implementation is not in compliance.

Recommended (or should)(S).

– These features add functionality supported by Core Architecture and should be implemented. Recommended features take advantage of the capabilities Core Architecture, usually without imposing major increase of complexity. Notice that for compliance testing, if a recommended feature is implemented, it shall meet the specified requirements to be in compliance with these guidelines. Some recommended features could become requirements in the future. The phrase "should not" indicates behaviour that is permitted but not recommended.

Allowed (may or allowed)(O).

– These features are neither required nor recommended by Core Architecture, but if the feature is implemented, it shall meet the specified requirements to be in compliance with these guidelines.

DEPRECATED.

– Although these features are still described in this document, they should not be implemented except for backward compatibility. The occurrence of a deprecated feature during operation of an implementation compliant with the current document has no effect on the implementation’s operation and does not produce any error conditions. Backward compatibility may require that a feature is implemented and functions as specified but it shall never be used by implementations compliant with this document.

Conditionally allowed (CA)

– The definition or behaviour depends on a condition. If the specified condition is met, then the definition or behaviour is allowed, otherwise it is not allowed.

Conditionally required (CR)

– The definition or behaviour depends on a condition. If the specified condition is met, then the definition or behaviour is required. Otherwise the definition or behaviour is allowed as default unless specifically defined as not allowed.

Strings that are to be taken literally are enclosed in "double quotes".

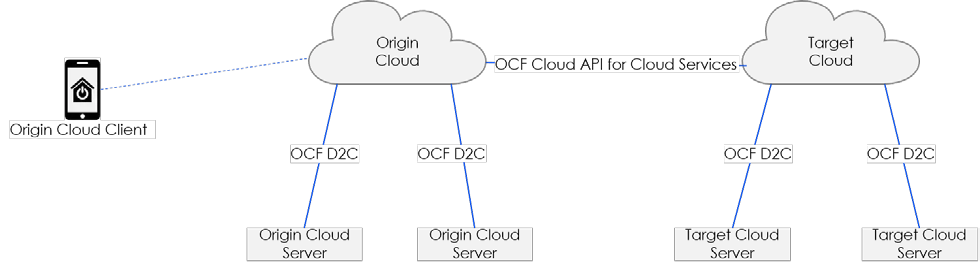
Words that are emphasized are printed in italic.

# 5 Обзор

## 5.1 Введение

Этот документ определяет OCF Cloud API для облачных сервисов. В этом документе Origin Cloud относится к облаку OCF или стороннему облаку, через которое пользователь работает со своими устройствами OCF, Target Cloud относится к облаку OCF, к которому подключены серверы OCF (устройства OCF), которыми пользователь хочет управлять через Origin Cloud.

Устройство OCF - это набор ресурсов, каждый из которых является объектом, определенным OpenAPI 2.0, который представляет физическое свойство или характеристику устройства (например, температуру, цвет света, выключатель питания). Само устройство имеет связанный тип устройства, который обеспечивает указание того, что это за устройство, например, свет представлен как тип устройства «oic.d.light».



См. Рисунок 1 для представления целевой архитектуры.

Рисунок 1 - Обзор облака OCF

OCF Cloud API для облачных сервисов поддерживает следующие случаи:

* API связывания аккаунтов (пункт 7)
* Первоначальная привязка учетной записи
* Удаление привязанного аккаунта
* API устройств (пункт 8)
* Извлечение всех устройств, связанных с пользователем (пункт 8.3)
* Получение одного устройства, связанного с пользователем (пункт 8.4)
* Получение единственного ресурса (пункт 8.5)
* Обновление одного Ресурса (п. 8.6)
* API событий (пункт 9)
* Подписка на мероприятие: создание подписки (п. 9.4.1)
* Уведомление: событие, созданное при установленной подписке (пункт 9.4.3).

## 5.2 Согласование облачной архитектуры OCF с ISO IEC 17789

Ссылка ISO / IEC 17789 определяет эталонную архитектуру облачных вычислений (CCRA), которую можно описать с точки зрения одной из четырех архитектурных точек зрения; пользовательский, функциональный, реализация и развертывание. Из четырех точек зрения реализация и развертывание явно выходят за рамки ISO / IEC 17789.

OCF определяет облачную службу типа возможностей приложения, предоставляющую связь как услугу (CaaS) (ссылка на ISO / IEC 17788). Эта облачная услуга предоставляется поставщиком облачных услуг, механизмы, используемые поставщиком облачных услуг для управления своей общей облачной инфраструктурой, являются вне области облачной службы, определенной OCF. Определение OCF специфично для интерфейса, предлагаемого облачной службой потребителю облачной службы, в частности пользователю облачной службы.

Определены три различных пользовательских представления. В случае, если заказчик облачной услуги является устройством OCF, как указано в разделе «Устройство OCF для облачных служб», то предоставляются следующие представления:

- Интерфейс для устройства OCF для предоставления информации облачной службе

- Интерфейс для устройства OCF для получения информации, предоставленной облачной службе

В случае, если заказчик облачной услуги является другим экземпляром облачной услуги, как указано в этом документе, предоставляется следующее представление:

- Интерфейс для другого экземпляра облачной службы для извлечения и обновления информации, предоставляемой через облачную службу.

Облачная служба OCF относится конкретно к пользователю службы облачных вычислений, существует единственное применимое действие службы облачных вычислений - «Использование службы облачных вычислений», определенное в пункте 8.2.21 ISO / IEC 17789.

Учетные данные для пользователя облачной службы предоставляются с использованием OAUTH2.0, как определено в RFC 6749. Облачная служба либо сама по себе, либо с помощью внешнего сервера авторизации предоставляет токен-носитель, который требуется во всех запросах от всех пользователей облачных вычислений. См. Пункт 7 и OCF Cloud Security.

Все соединения между пользователем облака и облачной службой осуществляются через TLS с взаимной аутентификацией; см. пункт 7.1 OCF Cloud Security.

## 5.3 Общий OCF Cloud API для элементов облачных сервисов

OCF Cloud API для облачных сервисов - это RESTful API через HTTPS (IETF RFC 2818). API определяется с помощью OpenAPI 2.0.

Origin Cloud взаимодействует с Target Cloud с помощью доменного имени или URI, полученного при начальной настройке клиента OAuth 2.0 (IETF RFC 6749), описанной в пункте 7.

Связь между устройствами OCF и облаками OCF определяется в OCF Device to Cloud Services.

Все URI, представленные в параметре ссылки "href", присутствующем в любой полезной нагрузке, должны иметь форму "/ <deviceId> / <resourcehref>"; где <deviceId> - это идентификатор Устройства, указанный в свойстве «di» в «/ oic / d», а «resourcehref» - это «href» Ресурса, предоставленный Целевым Облаком.

Исходное облако должно получить токен носителя из целевого облака с использованием стандартных механизмов OAuth2.0 (IETF RFC 6749). Все последующие запросы от исходного облака к целевому облаку должны включать устройство OCF к облачным службам этот токен-носитель для данного пользователя.

Любые параметры запроса, полученные Origin Cloud в запросе от клиента OCF, должны быть переданы через чистый (т.е. являются частью URI) в любом запросе, который отправляется в целевое облако.

Каждый запрос может содержать необязательный заголовок HTTP Correlation-ID, который несет уникальное значение идентификатора, которое предоставляет ссылку на конкретную транзакцию или цепочку событий в целевом облаке. Если запрос действительно содержит заголовок Correlation-ID, Correlation-ID, заполненный тем же значением, должен присутствовать в любом ответе на этот запрос. Если запрос не содержит заголовка Correlation-ID, он должен присутствовать в ответе.

Все запросы должны включать заголовок HTTP Accept, за исключением DELETE (поскольку в ответе не ожидается никакой полезной нагрузки). Все запросы или ответы, которые несут контент, должны включать заголовок HTTP Content-Type. Как минимум должны поддерживаться медиа-типы «application / json» и «application / vnd.ocf + cbor». Если получатель запроса не может предоставить ответ, закодированный в соответствии с содержимым заголовка Accept, следует отправить ответ HTTP 406 (неприемлемый) в соответствии с IETF RFC 2818. При получении ответа 406 отправитель запрос может повторить попытку запроса, используя альтернативный Content-Type, если он поддерживается.

Любые ответы, отправленные облаком OCF, могут включать диагностические данные (см. ИСО / МЭК 30118-1). Если диагностическая полезная нагрузка включена в ответ, ответ должен иметь заголовок Content-Type, закодированный как «текст / простой», см. Также пункт 6.6 IETF RFC 8075.

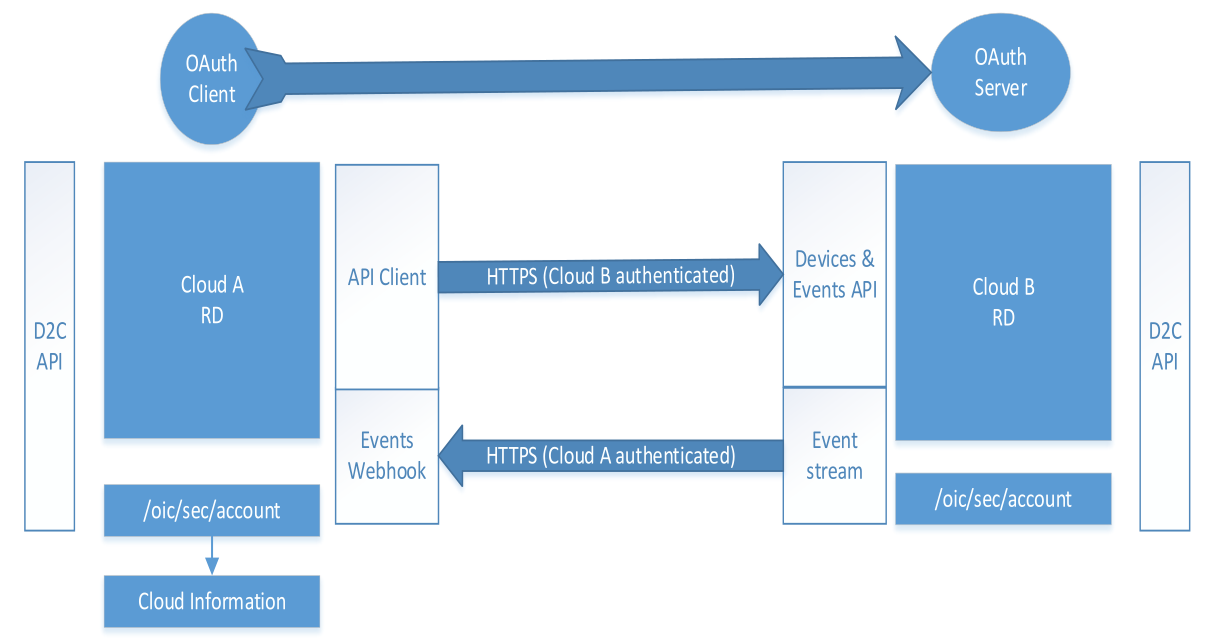
## 5.4 Обзор работы из облака в облако

### 5.4.1 Введение

В этом разделе представлен информативный обзор потоков, которые активируются подробным API, определенным в разделах 6, 7, 8 и 9. В разделе 5.4 приведены ссылки на применимые разделы в этом документе, которые определяют особенности API.

### 5.4.2 Концептуальная архитектура

На рисунке 2 представлена общая концептуальная архитектура..

Рисунок 2 - Концептуальная архитектура

### 5.4.3 Авторизация подключения к облаку

Рассмотрим пользователя, у которого есть учетные записи в двух разных, отдельно принадлежащих облаках, и устройства, связанные с каждой из этих учетных записей в этих облаках. Пользователь хочет иметь единое представление обо всех своих устройствах с одного клиента, а не иметь клиента на каждое облако. Пользователь через клиента, которого он хочет использовать для всех устройств, указывает напрямую подключенному облаку (Origin Cloud), что он хочет связать эту учетную запись с учетной записью в другом облаке (Target Cloud). Это инициирует стандартный поток типа предоставления кода авторизации OAuth2.0, см. IETF RFC 6749, пункт 1.3.1. Применение этого потока описано в разделе 7.

### 5.4.4 Синхронизация набора устройств пользователя

После завершения потока типа предоставления кода авторизации из пункта 5.4.3 Origin Cloud (то есть облако, к которому подключен пользователь) получает право использовать API устройства для получения от имени пользователя полного списка устройств, размещенных на Target Cloud, к которому у пользователя есть доступ. API описан в разделе 8, а последовательность операций дополнительно проиллюстрирована в разделе A.4.

Результатом вызова Device API является полный набор информации об устройстве, который затем может быть предоставлен в ответ на RETRIEVE на "/ oic / res" из Origin Cloud.

### 5.4.5 Сохранение актуальности: уведомления об изменениях в других облаках

После получения набора устройств Origin Cloud может подписаться на события, в которых оно заинтересовано, для всего набора устройств пользователя ("/ devices") или для каждого устройства в этом наборе ("/ devices / {deviceid}" ). См. Раздел 9 для получения подробной информации о самом API.

Подписка на «/ devices» позволяет Origin Cloud получать уведомления о добавлении нового устройства или удалении существующего из Target Cloud.

Подписка на "/ devices / {deviceid}" позволяет Origin Cloud получать уведомления об изменении состояния устройства (например, его снятие с регистрации).

Когда новое Устройство регистрируется в Target Cloud и существует подписка на это событие, в Origin Cloud отправляется уведомление с типом события «devices\_registered» и полезной нагрузкой, которая содержит «di» вновь зарегистрированного устройства. Затем Origin Cloud может ПОЛУЧИТЬ ссылки, предоставленные вновь добавленным устройством, используя "/ devices / {deviceid}", где "deviceid" был указан в полезной нагрузке уведомления. См. Раздел A.10 для последовательности операций, иллюстрирующих это взаимодействие.

### 5.4.6 Обработка запросов и ответов для подключенных устройств

С точки зрения клиента, подключенного к Origin Cloud, нет различия между устройствами и их ресурсами, размещенными в самом Origin Cloud, и устройствами и их ресурсами, которые размещены в Target Cloud, доступном через этот API.

Таким образом, все запросы к целевому ресурсу формируются с использованием механизмов, описанных в OCF Device to Cloud Services.

Облако Origin идентифицирует Целевое Облако для запрошенного Ресурса через «deviceid» в URI запроса, которое сопоставляется со свойством «di» в «/ oic / sec / account». Затем запрос эффективно передается в Целевое Облако через API "/ devices / {deviceid} / {resourcehref}", предоставляемый Целевым Облаком (см. Пункты 8.5 и 8.6). Любые параметры запроса, полученные через устройство для подключения к облаку, включаются в URI без изменений. Учитывается тип содержимого полезной нагрузки в запросе или ответе. См. Разделы A.6 и A.7 для иллюстративных потоков этого механизма для случаев RETRIEVE и UPDATE.

# 6 Аутентификация и авторизация

Целевое облако должно предоставлять только защищенные конечные точки; любые запросы, полученные через незащищенное соединение (например, HTTP), должны быть перенаправлены на безопасный эквивалент этой конечной точки. Исходное облако должно использовать схему аутентификации «Несущий» в поле заголовка запроса «Авторизация» для передачи маркера доступа в соответствии с пунктом 2.1 IETF RFC 6750. Для определения поля заголовка запроса «Авторизация» см. IETF RFC 2818.

Токены на предъявителя, выпущенные Target Cloud, должны идентифицировать пользователя, а также клиента, который отправляет запросы от имени пользователя в Target Cloud.

На стороне сервера OCF нет различий между запросами, пересылаемыми из Origin Cloud, и запросами, поступающими через Target Cloud.

# 7 API связывания аккаунтов

## 7.1 Общие

API привязки учетных записей - это механизм, с помощью которого устройства, размещенные от имени пользователя в Target Cloud, связываются с идентификатором пользователя в Origin Cloud. Установлена привязка аккаунта исключительно между исходным облаком и целевым облаком; Origin Cloud не должен проксировать устройства из Target Cloud в другое стороннее облако.

Клиент OAuth 2.0 Origin Cloud должен быть зарегистрирован в Target Cloud в качестве предварительного условия для запуска потока типа предоставления кода авторизации, который позволяет пользователю связать свою учетную запись Origin Cloud с Target Cloud. Этот процесс называется регистрацией приложения OAuth и выходит за рамки этого документа. Успешная регистрация клиента OAuth 2.0 Origin Cloud в целевом облаке зависит от двух объектов, устанавливающих доверительные отношения и получения требуемых параметров клиента и конечных точек токена OAuth2,0 (например, идентификатор клиента, секрет клиента, разрешенные URI перенаправления). См. IETF RFC 6749, пункт 2.

Связывание затем достигается за счет использования типа предоставления кода авторизации OAuth2.0. Частью процесса связывания является согласие конечного пользователя, что очень важно для междоменной федерации удостоверений, гарантируя, что злонамеренный облачный клиент OAuth 2.0 Origin не сможет получить авторизацию без ведома и явного согласия владельца ресурса (то есть пользователя ) целевого облака. Целевое облако представляет пользователю, связывающему учетную запись, точный объем информации для авторизации, запрашиваемой Клиентом. Подробная информация об объемах доступна в п. 7.2. После согласия пользователя и последующего обмена кодами авторизации токен-носитель и токены обновления (см. IETF RFC 6749) должны быть получены из целевого облака облаком происхождения в соответствии с форматом и типом контента в пункте 4 IETF RFC 6750. Токен-носитель идентифицирует личность пользователя в Target Cloud. Все запросы на токен-носитель или токен обновления должны включать «client\_id» и «client\_secret», как определено IETF RFC 6749. В пункте 2.3.1 IETF RFC 6749 описываются две схемы для включения «client\_id» и «client\_secret», одна с использованием заголовка авторизации с «базовой» схемой и заголовка, который кодирует учетные данные клиента в теле запроса, что не рекомендуется указанным RFC. Клиент должен предоставлять заголовок авторизации в запросах, использующих «Базовую» схему, Клиент не должен кодировать информацию в теле запроса.

Целевое облако может использовать область «offline\_access», как определено IETF RFC 7628, в таком случае Клиент, запрашивающий токен из такого целевого облака, должен включить область в запрос токена. То, как Клиент определяет, какие области целевого облака поддерживает или не поддерживает, выходит за рамки этого документа.

Параметр запроса «состояние» должен присутствовать в каждом запросе авторизации, см. Пункт 4.1.1 IETF RFC 6749. Состояние - это непрозрачное значение, используемое клиентом Origin Cloud для поддержания состояния между запросом и обратным вызовом во время процесса связывания учетной записи, см. Пункт A.3.

Все запросы, ответы и коды ошибок, которые могут быть отправлены во время связывания учетной записи, должны соответствовать тем, которые определены в RFC 6749.

Как только такой токен-носитель будет получен, Origin Cloud свяжет токен доступа и обновления OAuth2.0 со своим известным локальным «идентификатором пользователя». Пользователь, который связал свою учетную запись Target Cloud с учетной записью Origin Cloud, с этого момента может запрашивать все свои устройства через Origin Cloud, поскольку Origin Cloud может отправлять запросы в Target Cloud от имени учетной записи пользователя Target Cloud. Однако, если исходное облако делает запрос, который не входит в область действия токена доступа OAuth2.0, предоставленную токеном носителя, целевое облако должно ответить соответствующим ответом об ошибке.

При первом получении токена-носителя рекомендуется, чтобы Origin Cloud использовала API устройства для получения сведений об устройстве для всех устройств в области токена доступа OAuth2.0 для токена-носителя.

Если Origin Cloud поддерживает поведение, определенное в OCF Device to Cloud Services, то, как только Origin Cloud получит набор устройств из целевого облака, оно создает экземпляр «/ oic / sec / account» для каждого устройства. Необязательное свойство «cloudid» в «/ oic / sec / account» устанавливается равным UUID облака OCF целевого облака, доступному в поле «Общее имя» сертификата конечного объекта. Если Свойство отсутствует, пусто или содержит то же значение, что и UUID Origin Cloud, значит, Устройство является локальным для Origin Cloud.

Origin Cloud может использовать API событий для установления подписки с Устройствами в Целевом облаке; таким образом, чтобы добавление или удаление устройств в целевом облаке можно было правильно отразить в Origin Cloud. Когда устройство снимается с регистрации в целевом облаке, оно становится недоступным через Origin Cloud. Когда токен носителя, полученный из целевого облака, истекает, а токен обновления все еще действителен, Origin Cloud может запросить новый токен носителя через конечную точку маркера OAuth2.0 целевого облака. Когда срок действия токена обновления истекает, он недоступен или токен-носитель не может быть получен, Origin Cloud удаляет все ассоциации с Устройствами, размещенными в Target Cloud. Дополнительные сведения см. В IETF RFC 6749.

Рекомендуется, чтобы Origin Cloud подписывалась на события каждого Устройства, размещенного в Target Cloud, с помощью механизма подписки, описанного в пункте 9.6.

## 7.2 Области действия токена доступа OAuth2.0

В этом документе определяется базовый набор областей токенов доступа OAuth2.0, см. IETF RFC 6749. Origin Cloud может запрашивать одну или несколько из этих областей, ее расширение поставщика или конкретную область действия поставщика как часть привязки учетной записи. процесс. Если область действия, предоставляемая Целевым облаком, отличается от запрошенной области, то эта область должна быть включена в выданный маркер доступа (см. Пункт 5.1 IETF RFC 6749). Если целевое облако поддерживает запросы токенов доступа без предоставленных областей, и запрос токена доступа без областей действия получен от Origin Cloud, то возвращенный токен доступа из целевого облака должен предоставить доступ ко всем областям токенов доступа OAuth2.0. определено в таблице 1.

Описание для каждой области токена доступа OAuth2.0 должно быть представлено пользователю в процессе связывания учетной записи сервером OAuth2.0 целевого облака. Пользователь Target Cloud видит описание на экране согласия и дает явное согласие на то, что Origin Cloud, запрашивающий токен-носитель, уполномочен действовать от имени пользователя в пределах полученных областей действия токена доступа OAuth2.0.

Таблица 1 - Области действия токенов доступа OAuth 2.0

|  |  |
| --- | --- |
| OAuth2.0 access token scope name | OAuth2.0 access token scope description "The application will be able to:" |
| r:\* | Read |
| w:\* | Update |

В таблице 2 подробно описаны области маркеров доступа OAuth2.0, применимые для каждой конечной точки API. Все конечные точки API, перечисленные в таблице 2, должны поддерживаться целевым облаком. Так, например, если Origin Cloud отправляет запрос GET в конечную точку API "/ api / v1 / devices? Content = all", у Origin Cloud должен быть токен носителя, который содержит область действия токена доступа OAuth2.0 "r: \*" или его расширение поставщика

Таблица 2 - Применимые области токенов доступа OAuth2.0 для каждой конечной точки API

|  |  |  |
| --- | --- | --- |
| API Endpoint | HTTP Request type | Applicable scopes |
| /api/v1/devices | GET | r:\* |
| /api/v1/devices?content=all | GET | r:\* |
| /api/v1/devices/{deviceid} | GET | r:\* |
| /api/v1/devices/{deviceid}?content=all | GET | r:\* |
| /api/v1/devices/{deviceid}/{resourcehref} | GET | r:\* |
|  |  |  |
| POST | w:\* |
| /api/v1/devices/subscriptions | POST | r:\* |
| DELETE | r:\* |
| /api/v1/devices/{deviceid}/subscriptions | POST | r:\* |
| DELETE | r:\* |
| /api/v1/devices/{deviceid}/{resourcehref}/subscriptions | POST | r:\* |
| DELETE | r:\* |

Поставщик может расширить список областей действия токена доступа OAuth2.0 за пределы перечисленных в таблице 2. Они расширяются путем добавления дополнительной специфической информации поставщика перед \* в имени области действия токена доступа OAuth2.0 (например, «r: xyz: \* "). Как работают эти расширения, выходит за рамки OCF, но они могут присутствовать в запросе токена доступа OAuth2.0. Обратите внимание, что если пользователь дает согласие Origin Cloud на «w: \*», согласие применяется также к любым производным областям токенов доступа OAuth2.0 (например, «w: xyz: \*»).

# 8. API устройств

## 8.1 Введение

API устройств поддерживает возможность извлечения и взаимодействия с устройствами OCF, находящимися внутри

объем предоставленного токена на предъявителя.

## 8.2 Параметры, поддерживаемые в запросах

В таблице 3 перечислены параметры, которые могут быть предоставлены как часть запроса в API устройства.

Таблица 3 - Параметры, используемые в запросах в API устройства

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Friendly Name | Parameter Name | Location | Mandatory | Description |
| Accept | Accept | HTTP Header | Yes | An Accept request HTTP header advertises which content types, expressed as MIME types, the Origin Cloud is able to understand.  The Target Cloud then selects one of the proposed content types and informs the Origin Cloud of its choice with the Content-Type response header. |
| Content Type | Content-Type | HTTP Header | No | The Content-Type header is used to indicate the media type of the payload. A Content-Type header tells the recipient what the content type of the returned payload actually is. |
| Correlation ID | Correlation-ID | HTTP Header | No | A Correlation ID, also known as a Transit ID, is a unique identifier value that is attached to requests and messages that allows reference to a particular transaction or event chain. |
| Content | content=[base, all] | Query String Parameter | No | When set to "base" this indicates to the recipient that |
|  |  |  |  | the response payload Links are not resolved.  When set to "all" this indicates to the recipient that the response payload is the resolved (i.e. resource representation) Link and not the Link itself. If not present "base" is assumed. |

## 8.3 Получить все устройства

### 8.3.1 Резюме

Этот запрос отправляется из Origin Cloud в целевое облако, чтобы получить информацию обо всех устройствах, зарегистрированных для пользователя, которые входят в область действия, определенную токеном-носителем в целевом облаке.

Запрос к этому API может быть вызван Origin Cloud после завершения привязки учетной записи. Если облако поддерживает поведение, определенное в OCF Device to Cloud Services, это также может быть вызвано получением RETRIEVE в «/ oic / res» каталога облачных ресурсов от клиента OCF.

В таблице 4 представлена сводка API.

Таблица 4 - Сводка по API "Получить все устройства

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HTTP  Request Type | API Endpoint | Parameters | Response Code | Response Payload |
| GET | /api/v1/devices | content=[base, all],  Correlation-ID, Accept | 200 | See clause [B.1](#_bookmark176) - array of  /definitions/Device (for content=base) and  /definitions/DeviceContentAll (for content=all) |
| 400, 401, 403,  503, 504 | The response may include a diagnostic payload  containing a reason string. |

### 8.3.2 Полезные данные запроса и ответа

В запросе нет требуемой полезной нагрузки; если он получен в Целевом облаке, он игнорируется. Необходимая полезная нагрузка ответа для запроса, который включает параметр «content = base» или не содержит параметр «content», должна быть массивом объектов; каждый объект должен содержать Свойства, определенные в схеме, представленной в Приложении B, Свойство «устройство», как определено схемой, Свойство статуса («статус»), которое указывает, находится ли Устройство в сети или офлайн, и массив ссылок ( как определено для "/ oic / res") для Ресурсов, предоставляемых конкретным Устройством. Эти свойства приведены в таблице 5, а конкретные свойства свойства «устройство» приведены в таблице 6.

Таблица 5 - Определение свойства полезной нагрузки ответа

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Property title | Property name | Value type | Value rule | Unit | Access mode | Mandatory | Description |
| Device | "device" | "object" | N/A | N/A | R | Yes | Set of Properties that  defined the Device itself; see Table YYYY |
| Device Status | "status" | "string: | Value from the enumeration  {"online","offline"} | N/A | R | Yes | Status of the Device. |
| Device Links | "links" | "array" | N/A | N/A | R | Yes | The published set of Links exposed by the Device |

Table 6 – "device" Property definition

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Property title | Property name | Value type | Value rule | Unit | Access mode | Mandatory | Description |
| Resource Type | "rt" | "array" | N/A | N/A | R | Yes | Array contained the Device Type of the Device |
| (Device) Name | "n" | "string: | N/A | N/A | R | Yes | Human friendly name defined by the vendor. |
| Device UUID | "di" | "uuid" | N/A | N/A | R | Yes | Unique identifier for Device. |
| Manufacturer Name | "dmn" | "array" | N/A | N/A | R | Yes | Name of manufacturer of the  Device, in one or more languages. This Property is an array of objects where each object has a  "language" field (containing an [IETF RFC 5646](#_bookmark4) language tag) and a "value" field containing the  manufacturer name in the indicated language. |

Минимальный набор доступных ресурсов зависит от типа устройства OCF; это должен быть набор, определенный в пункте 6.1.3.2.1 OCF Device to Cloud Services.

Если запрос включает «content = all» (аналогично пакетному извлечению / oic / res в ближайшей сети), то полезная нагрузка ответа должна быть такой, как определено для «content = base», за исключением того, что вместо массива ссылок на размещенных Ресурсов, полезная нагрузка ответа должна включать в себя массив представлений самих Ресурсов, которые доступны для каждого доступного Устройства. Это проиллюстрировано в примерах, представленных для API устройства в Приложении B. См. Также определение пакетного ответа в ISO / IEC 30118-1.

### 8.3.3 Ответы

В случае успеха будет предоставлен ответ 200. Полезная нагрузка должна содержать информацию для всех устройств, которые входят в область действия токена-носителя.

Неуспешный ответ пути, указывающий на тип ошибки, должен быть возвращен Целевым Облаком, если обнаружен сценарий ошибки. В Таблице 7 перечислены возможные неуспешные ответы на пути и возможные сценарии, запускающие их генерацию; реализация может поддерживать дополнительные ответы, как определено в IETF RFC 2818.

Таблица 7 - Отклики неуспешного пути API устройств

|  |  |
| --- | --- |
| Response Code | Response scenario |
| 400 | May be sent by the Target Cloud if the request was malformed or badly constructed |
| 401 | May be sent by the Target Cloud if the request is unauthorized (e.g. an invalid or missing Bearer Token) |
| 403 | May be sent by the Target Cloud if the requestor is known however the OAuth2.0 Access Token Scope of the request is forbidden |
| 406 | May be sent by the Target Cloud if the media type in the received Accept header is not supported/acceptable |
| 503 | May be sent by the Target Cloud if the service on the Target Cloud is unavailable |
| 504 | May be sent by the Target Cloud if the target Device is registered at the Target Cloud, however the Device itself is unavailable, offline, or otherwise unreachable. The response should include a Retry-After header containing the time after which the request may be re-attempted. Additional information may be indicated in a diagnostic payload |

8.4 Получить одно устройство

8.4.1 Резюме

Этот запрос может быть отправлен из исходного облака в целевое облако для получения информации об определенном устройстве, которое зарегистрировано для пользователя, попадающего в область действия, определенную токеном носителя в целевом облаке.

Запрос к этому API может быть вызван в Origin Cloud после получения уведомления о том, что новое Устройство было добавлено в партнерское облако, или, альтернативно, как часть потока после связывания учетной записи. Если Origin Cloud поддерживает OCF Device to Cloud Services, запрос к этому API также может быть вызван после получения RETRIEVE в «/ oic / res» каталога ресурсов Origin Cloud от клиента OCF с параметром запроса, который указывает конкретный "deviceid" (т.е. "? anchor = ocf: // <некоторый uuid устройства>").

В таблице 8 представлена сводка API.

Таблица 8 - Получение сводки API одного устройства

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HTTP  Request Type | API Endpoint | Parameters | Response Code | Response Payload |
| GET | /api/v1/devices/{deviceid} | content=[base,  all],  Correlation-ID, Accept | 200 | See clause [B.1](#_bookmark176) -  /definitions/Device (for content=base) and /definitions/DeviceConten tAll (for content=all) |
| 400, 401,  403, 404,  503, 504 | The response may include a diagnostic payload containing a reason string |

### 8.4.2 Полезные данные запроса и ответа

В запросе нет требуемой полезной нагрузки; если он получен в Целевом облаке, он игнорируется.

«Deviceid» в URI запроса совпадает со свойством «di» из / oic / d целевого устройства OCF.

Полезная нагрузка ответа должна быть объектом, содержащим обязательную информацию об устройстве, как определено в пункте 8.3.2.

### 8.4.3 Ответы

В случае успеха будет предоставлен ответ 200. Полезная нагрузка должна содержать информацию о запрошенном Устройстве.

Неуспешный ответ пути, указывающий на тип ошибки, должен быть возвращен Целевым Облаком, если обнаружен сценарий ошибки. В таблице 9 перечислены возможные неуспешные ответы пути и возможные сценарии, которые могут вызвать их генерацию; реализация может поддерживать дополнительные ответы, как определено в IETF RFC 2818.

Таблица 9 - Ответы на неудачный путь API устройства

|  |  |
| --- | --- |
| Response Code | Response scenario |
| 400 | May be sent by the Target Cloud if the request was malformed or badly constructed |
| 401 | May be sent by the Target Cloud if the request is unauthorized (e.g. an invalid or missing Bearer Token) |
| 403 | May be sent by the Target Cloud if the requestor is known however the OAuth2.0 Access Token Scope of the request is forbidden |
| 404 | May be sent by the Target Cloud if the indicated "deviceid" is not present on the Target Cloud |
| 406 | May be sent by the Target Cloud if the media type in the received Accept header is not supported/acceptable |
| 503 | May be sent by the Target Cloud if the service on the Target Cloud is unavailable |
| 504 | May be sent by the Target Cloud if the target Device is registered at the Target Cloud, however the Device itself is unavailable, offline, or otherwise unreachable. The response should include a Retry-After header containing  the time after which the request may be re-attempted. Additional information may be indicated in a diagnostic payload |

## 8.5 Получение определенного ресурса

### 8.5.1 Резюме

Этот запрос отправляется из Origin Cloud в целевое облако для получения информации о конкретном ресурсе, который предоставляется устройством, зарегистрированным для пользователя, входящего в область действия, определенную токеном-носителем в целевом облаке.

Если облако поддерживает подключение устройства OCF к облачным службам, это может быть инициировано получением RETRIEVE на URI, предоставленный ссылкой в каталоге облачных ресурсов от клиента OCF. В таблице 10 представлена сводка API.

Таблица 10 - Получение сводки API конкретных ресурсов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HTTP  Request Type | API Endpoint | Parameters | Response Code | Response Payload |
| GET | /api/v1/devices/{deviceid}/{resourcehref} | Correlation-ID, Accept | 200 | Response payload as defined by OCF for the target  Resource Type |
|  |  |  | 400, 401,  403, 404 | The response may include a  diagnostic payload containing a  reason string |
| 503 | The response may include a  diagnostic payload containing a  reason string |
| 504 | Retry-After header and optionally a  diagnostic payload containing a  reason string. |

### 8.5.2 Полезные данные запроса и ответа

В запросе нет требуемой полезной нагрузки; если он получен в Целевом облаке, он игнорируется.

«Deviceid» в URI в запросе совпадает со свойством «di» из «/ oic / d» целевого устройства OCF. «Resourcehref» в URI совпадает с параметром ссылки «href» для целевого экземпляра ресурса 667.

Полезная нагрузка ответа должна быть такой, как определено OCF для получаемого Ресурса, или как определено поставщиком, если Ресурс является Ресурсом третьей стороны.

Учитывается тип содержимого полезной нагрузки ответа, полученной от целевого сервера; то есть контент и полезная нагрузка, полученные Целевым Облаком, должны быть проксированы без изменений в ответе. Таким образом, например, в случае, когда целевой сервер является устройством OCF, тип содержимого будет «application / vnd.ocf + cbor».

Исходное облако должно включать неизмененные в requestURI запроса, отправленного в целевое облако, любые параметры запроса, полученные через устройство для подключения к облаку.

### 8.5.3 Ответы

В случае успеха будет предоставлен ответ 200. Полезная нагрузка в ответе должна быть такой, как определено на http://oneiota.org для целевого типа ресурса.

Неуспешный ответ пути, указывающий на тип ошибки, должен быть возвращен TargetCloud, если обнаружен сценарий ошибки. В таблице 11 перечислены возможные неуспешные ответы пути и возможные сценарии, которые могут вызвать их генерацию; реализация может поддерживать дополнительные ответы, как определено в IETF RFC 2818.

Таблица 11 - Ответы на неудачный путь API извлечения ресурсов

|  |  |
| --- | --- |
| Response Code | Response scenario |
| 400 | May be sent by the Target Cloud if the request was malformed or badly constructed |
| 401 | May be sent by the Target Cloud if the request is unauthorized (e.g. an invalid or missing Bearer Token) |
| 403 | May be sent by the Target Cloud if the requestor is known however the OAuth2.0 Access Token Scope of the request is forbidden |
| 404 | May be sent by the Target Cloud if the indicated "deviceid" is not present on the Target Cloud or the "resourcehref" is not found |
| 406 | May be sent by the Target Cloud if the media type in the received Accept header is not supported/acceptable |
| 503 | May be sent by the Target Cloud if the service on the Target Cloud is unavailable |
| 504 | May be sent by the Target Cloud if the target Device is registered at the Target Cloud, however the Device itself is unavailable, offline, or otherwise unreachable. The response should include a Retry-After header containing  the time after which the request may be re-attempted. Additional information may be indicated in a diagnostic payload |

## 8.6 Обновление ресурса на устройстве

### 8.6.1 Резюме

Этот запрос отправляется из Origin Cloud в целевое облако, чтобы обновить информацию, содержащуюся в конкретном Ресурсе, предоставляемом Устройством, которое зарегистрировано для пользователя, который входит в область действия, определенную токеном носителя в Целевом облаке.

Если Облако поддерживает OCF Device to Cloud Services, запрос к этому API может быть инициирован получением UPDATE для URI, предоставленного ссылкой в Каталоге облачных ресурсов от клиента OCF.

В таблице 12 представлена сводка API.

Таблица 12 - Сводка API ресурсов обновления

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HTTP  Request Type | API Endpoint | Parameters | Response Code | Response Payload |
| POST | /api/v1/devices/{deviceid}/{resourcehref} | payload, | 200 | Optional resource |
|  |  | Correlation-ID, |  | representation |
|  |  | Accept, Content- | 400, 401, | The response may |
|  |  | Type | 403, 404, | include a diagnostic |
|  |  |  | 415 | payload containing a |
|  |  |  |  | reason string. |
|  |  |  | 503 | The response may |
|  |  |  |  | include a diagnostic |
|  |  |  |  | payload containing a |
|  |  |  |  | reason string. |
|  |  |  | 504 | Retry-After header and |
|  |  |  |  | optionally a diagnostic |
|  |  |  |  | payload containing a |
|  |  |  |  | reason string |

### 8.6.2 Полезные данные запроса и ответа

Полезная нагрузка запроса должна быть такой, как определено OCF для обновляемого ресурса, или как определено поставщиком, если ресурс является сторонним ресурсом.

«Deviceid» в URI в запросе совпадает со свойством «di» из / oic / d целевого устройства OCF. «Resourcehref» в URI совпадает с параметром ссылки «href» для целевого экземпляра ресурса.

Полезная нагрузка ответа должна быть такой, как определено OCF для получаемого Ресурса, или как определено поставщиком, если Ресурс является Ресурсом третьей стороны.

Content-Type запроса определяется в заголовке Content-Type HTTP. В случае, если запрос был инициирован другим устройством OCF, значение заголовка формата содержимого CoAP должно быть преобразовано в заголовок HTTP Content-Type в целевое облако. Если значение отсутствует, Target Cloud пересылает запрос как есть. Таким образом, например, в случае, когда клиент-источник является устройством OCF, параметром формата содержимого CoAP будет «application / vnd.ocf + cbor», который передается в целевое облако как заголовок HTTP Content-Type.

Исходное облако должно включать неизмененные в requestURI запроса, отправленного в целевое облако, любые параметры запроса, полученные через устройство для подключения к облаку.

### 8.6.3 Ответы

В случае успеха будет предоставлен ответ 200. Полезная нагрузка может дополнительно содержать представление обновленного ресурса.

Неуспешный ответ пути, указывающий на тип ошибки, должен быть возвращен Целевым Облаком, если обнаружен сценарий ошибки. В таблице 13 перечислены возможные неуспешные ответы пути и возможные сценарии, которые могут вызвать их генерацию; реализация может поддерживать дополнительные ответы, как определено в IETF RFC 2818.

719 Таблица 13 - Ответы на неудачный путь API обновления ресурсов

|  |  |
| --- | --- |
| Response Code | Response scenario |
| 400 | May be sent by the Target Cloud if the request was malformed or badly constructed |
| 401 | May be sent by the Target Cloud if the request is unauthorized (e.g. an invalid or missing Bearer Token) |
| 403 | May be sent by the Target Cloud if the requestor is known however the OAuth2.0 Access Token Scope of the request is forbidden |
| 404 | May be sent by the Target Cloud if the indicated "deviceid" is not present on the Target Cloud or the "resourcehref" is not found |
| 406 | May be sent by the Target Cloud if the media type in the received Accept header is not supported/acceptable |
| 415 | May be sent by the Target Cloud if an unsupported media type was specified in the Content-Type header |
| 503 | May be sent by the Target Cloud if the service on the Target Cloud is unavailable |
| 504 | May be sent by the Target Cloud if the target Device is registered at the Target Cloud, however the Device itself is unavailable, offline, or otherwise unreachable. The response should include a Retry-After header containing  the time after which the request may be re-attempted. Additional information may be indicated in a diagnostic payload |

# 9 API событий

## 9.1 Введение

API событий поддерживает возможность для заинтересованной стороны подписываться на события и впоследствии получать уведомления об этих событиях. События могут быть на уровне ресурсов (например, наблюдение CoAP) или на более системном уровне (например, при изменении набора известных устройств).

API событий использует механизм, с помощью которого Target Cloud уведомляет Origin Cloud о возникновении нового события в Target Cloud или на любом устройстве, связанном с Target Cloud. Этот поток событий (непрерывная серия уведомлений) может быть запущен путем отправки первоначального запроса подписки в целевое облако с указанием «eventTypes», «eventsUrl» (конечная точка API, на которую отправляются уведомления) и «signatureSecret», последний для проверить подлинность запросов от Target Cloud. См. Пункт 9.2. для получения подробных сведений о механизме использования «signatureSecret» и в пункте 9.4.1 для получения более подробной информации о запросе подписки.

Идентификатор подписки должен быть предоставлен в ответ на первоначальный запрос подписки. Идентификатор подписки - это уникальная строка типа UUID, которая должна быть создана и сохранена Целевым облаком. Созданный идентификатор должен быть частью каждого уведомления, отправляемого на настроенный «eventsUrl». Идентификатор подписки также используется для УДАЛЕНИЯ этой подписки. Идентификатор подписки либо присутствует в полезных данных ответа, либо в заголовке HTTP, либо присутствует как часть URI запроса в зависимости от выполняемой операции. См. Разделы 9.4.2 и 9.4.3 для получения более подробной информации.

После успешной подписки Target Cloud отправит начальное уведомление в Origin Cloud «eventsUrl» (которое было предоставлено во время создания подписки) с текущим состоянием элементов, к которым применяется подписка. Target Cloud будет отправлять дополнительные уведомления в Origin Cloud всякий раз, когда происходят какие-либо изменения (т. Е. События) в элементах, к которым применяется подписка.

После успешной подписки Origin Cloud на события Target Cloud, Target Cloud начнет отправлять уведомления только после того, как установит новое аутентифицированное сервером TLS-соединение с «eventsUrl», как указано в Target Cloud.

Уведомления, генерируемые Target Cloud в ответ на подписку, должны быть только для устройств и изменений системы, которые авторизует Bearer Token.

## 9.2 Аутентификация событий

### 9.2.1 Введение

Подписи на основе хеш-кода аутентификации сообщений (HMAC) - это способ подписать данные уведомления с помощью «signatureSecret», которое знают только Origin Cloud и Target Cloud. «SigningSecret» создается Origin Cloud и отправляется в запросе подписки, как определено в пункте 9.4.1. После успешной подписки Целевое Облако должно подписывать каждое уведомление, используя алгоритм хеширования HMAC-SHA256, следуя формуле из пункта 9.2.2. Вычисленная подпись должна быть прикреплена как заголовок «Event-Signature» к каждому запросу на уведомление, отправляемому в Origin Cloud.

Подпись будет использоваться Origin Cloud для проверки легитимности источника и самих данных. Когда уведомление получено Origin Cloud, оно должно использовать свой сохраненный секрет и уведомление для генерации собственной подписи HMAC-SHA256, используя формулу из пункта 9.2.1 для сравнения со значением из заголовка «Event-Signature».

Если секрет подписи и запрос уведомления совпадают с обеих сторон, подпись HMAC будет совпадать. Этот матч подтверждает подлинность запроса и данных.

Если подпись HMAC не совпадает, Origin Cloud игнорирует запрос уведомления.

сообщение.

Подробный обзор представлен в A.8.2, A.9.2, A.10.2 и A.11.2.

### 9.2.2 Создание подписи события

1) Получить текущую метку времени в формате времени Unix; это используется для заполнения "Event-Timestamp" заголовок.

2) Создайте строку, состоящую из конкатенации закодированного содержимого следующих заголовков, которые являются частью уведомления, которое должно быть отправлено, в следующем порядке: «Content-Type», «Event-Type», «Subscription». -ID »,« Порядковый номер »и« Отметка времени события ». Между каждым значением вставьте двоеточие (шестнадцатеричное значение символа ASCII 3A) в качестве разделителя. Если какой-либо из заголовков отсутствует, не включайте это значение, но все же включайте разделитель (например, если «Content-Type» отсутствует, включите «:» перед кодированием «Event-Type»). Все заголовки, которые определены как строки, должны обрабатываться как символы ASCII.

3) После кодирования «Event-Timestamp» добавьте последнее двоеточие (шестнадцатеричное значение символа ASCII 3A) и необработанные байты (т.е. те, которые будут включены в HTTP-запрос), составляющие тело уведомления, которое будет отправлено.

4) Хешируйте полученную строку, используя в качестве ключа «signatureSecret», используя алгоритм хеширования HMAC-SHA256 и взяв шестнадцатеричный дайджест хеша.

5) Включите полученную подпись в заголовок «Event-Signature» уведомления и отметку времени в заголовок «Event-Timestamp».

### 9.2.1 Проверка подписи события

1) Создайте строку, которая состоит из конкатенации закодированного содержимого следующих заголовков 786, полученных в уведомлении, в следующем порядке: «Content-Type», «Event-Type», «Subscription-ID», 787 ». Порядковый номер »и« Отметка времени события ». Между каждым значением вставьте двоеточие (символ ASCII 788, шестнадцатеричное значение 3A) в качестве разделителя. Если какой-либо из заголовков отсутствует, не включайте это значение, но 789 все еще включает разделитель (например, если «Content-Type» отсутствует, включите «:» до кодирования 790 «Event-Type»). Все заголовки, которые определены как строки, должны обрабатываться как символы ASCII.

2) После кодировки «Event-Timestamp» добавьте последнее двоеточие (шестнадцатеричное значение символа ASCII 3A) и

полученные необработанные байты (т.е. не подлежащие декодированию) тела уведомления.

3) Хешируйте полученную строку, используя в качестве ключа «signatureSecret», используя хеширование HMAC-SHA256.

алгоритм и возьмите шестнадцатеричный дайджест хэша.

4) Сравните созданную подпись с заголовком «Event-Signature» полученного уведомления и

убедитесь, что они совпадают.

### 9.3 Поддерживаемые параметры

В таблице 14 перечислены параметры, которые могут быть предоставлены в API событий.

Таблица 14 - Параметры, используемые в API событий

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Friendly Name | Parameter Name | Location | Mandatory | Description |
| Accept | Accept | HTTP Header | Yes except for  subscription cancellation (DELETE) | An Accept request HTTP header advertises which content types,  expressed as MIME types, the client is able to understand. The resource server then selects one of the proposal and  informs the client of its choice with the Content-Type response header. Each notification sent to the defined  "eventsUrl" is then using this Accepted content type. |
| Correlation ID | Correlation-ID | HTTP Header | No | A Correlation ID, also known as a Transit ID, is a unique identifier value that is  attached to requests and responses that allows reference to a particular  transaction or notification. |
| Content Type | Content-Type | HTTP Header | No | The Content-Type header is used to  indicate the media type of the payload. A Content-Type header tells the recipient what the content type of the returned  payload actually is. |

## 9.4 Подписка на API событий и определения полезной нагрузки уведомлений

### 9.4.1 Запрос подписки

Запрос подписки отправляется Origin Cloud в конечную точку API, определенную для типа события, на которое нацелена подписка. Набор типов событий и связанных конечных точек API представлен в таблице 15. Целевое облако должно поддерживать типы событий «resources\_published» и «resources\_unpublished», целевое облако должно поддерживать все другие типы событий, перечисленные в таблице 15. Если по какой-либо причине цель Облако не может удовлетворить запрос подписки на событие определенного типа, оно должно ответить соответствующим окончательным ответом пути неуспеха.

Подписка на событие типа subscription\_cancelled не выполняется Origin Cloud явно; он всегда должен быть включен в целевом облаке, когда любой другой поддерживаемый тип события является целевым подписки.

Таблица 15 - Типы событий и конечные точки API

|  |  |
| --- | --- |
| Event-Type | API Endpoint |
| subscription\_cancelled | N/A as a subscription\_cancelled event type is not explicitly subscribed to. |
| devices\_registered | /api/v1/devices/subscriptions |
| devices\_unregistered | /api/v1/devices/subscriptions |
| devices\_online | /api/v1/devices/subscriptions |
| devices\_offline | /api/v1/devices/subscriptions |
| resource\_contentchanged | /api/v1/devices/{deviceid}/{resourcehref}/subscriptions |
| resources\_published | /api/v1/devices/{deviceid}/subscriptions |
| resources\_unpublished | /api/v1/devices/{deviceid}/subscriptions |

Приложение B содержит определение полезной нагрузки, содержащейся в запросе подписки. Свойства, которые содержатся в полезной нагрузке, дополнительно поясняются в Таблице 16.

Таблица 16 - Свойства полезной нагрузки запроса подписки

|  |  |  |  |
| --- | --- | --- | --- |
| Payload Property Name | Value type | Mandatory | Description |
| eventsUrl | URI | Y | URI to which notifications are to be sent |
| eventTypes | array of enum | Y | Event type(s) for which the subscription is targeted.  See [Table 15](#_bookmark82) |
| signingSecret | String of length 32 | Y | Secret used to create HMAC signature for each event |

[Figure 3](#_bookmark84) is an example of such a payload.

**{**

**"eventsUrl": "**[**https://mynotificationuri**](https://mynotificationuri/)**", "eventTypes": ["resource\_contentchanged"], "signingSecret": "DVDUEBe5nciVSXU85BPxrAjSsHenTzWY"**

**}**

Рисунок 3 - Пример запроса подписки

### 9.4.2 Ответ подписки

Определение ответа на запрос подписки приведено в Приложении B. Свойства, содержащиеся в полезной нагрузке, дополнительно поясняются в Таблице 17.

Таблица 17 - Свойства ответа подписки

|  |  |  |  |
| --- | --- | --- | --- |
| Payload Property Name | Value type | Mandatory | Description |
| subscriptionId | Uuid | Y | Identity of the subscription (the Subscription ID). May be mapped from other  protocols if a unique  identifier exists. Note this cannot be mapped from a CoAP Token as the Token in CoAP is Client-local in scope (i.e. not guaranteed unique beyond the Client issuing the request). |

[Figure 4](#_bookmark87) is an example of such a payload.

Рисунок 4 - Пример полезной нагрузки ответа на подписку

**{**

**"subscriptionId": "1eeb465c-5e8d-4305-a366-bbf035fff671"**

**}**

### 9.4.3 Запрос уведомления

Когда подписка впервые успешно установлена, Target Cloud отправит запрос POST на «eventsUrl», который был предоставлен в подписке, с текущим состоянием элементов, к которым применяется подписка. Должен быть один запрос POST для каждого типа подписанного события; то есть, если запрос на подписку содержит несколько типов событий в свойстве «eventTypes», существует запрос уведомления для каждого идентифицированного типа события, а не один для всех типов событий.

Когда происходит последующее изменение (то есть событие), которое запускает уведомление, Target Cloud отправляет запрос POST на «eventsUrl», который был предоставлен в подписке. Целевое облако должно заполнять все заголовки, определенные в таблице 18 в POST, который отправляется на «eventsUrl», предоставленный исходным облаком, вместе с любыми полезными данными уведомления.

Целевое облако должно отправить уведомление с типом события «subscription\_cancelled» в «eventsUrl», предоставленном Origin Cloud, в случае отмены подписки. Поскольку нет определенной полезной нагрузки для события «subscription\_cancelled», запрос POST, отправляемый для этого типа события, не должен включать заголовок «Content-Type». Отмена может происходить путем приема DELETE от исходного облака (см. Пункты 9.4.4, 9.6 и 9.7) или посредством внутренней логики в самом целевом облаке.

Если запрос, установивший подписку, содержал заголовок Correlation-ID, то все уведомления, отправленные в результате этой подписки, должны содержать заголовок Correlation-ID, заполненный тем же значением, что и полученный в исходном запросе на подписку.

Таблица 18 - HTTP-заголовки запроса уведомления

|  |  |  |  |
| --- | --- | --- | --- |
| HTTP Header | Value Type | Mandatory | Description |
| Correlation-ID | UUID | No | A Correlation ID, also known as a Transit ID, is a unique identifier value that is attached to  requests and responses that allows reference to a particular transaction or event chain. |
| Content-Type | String | Yes, for  notifications  that include a payload | Indicates the media type of the notification payload |
| Event-Type | String | Yes | Type of the event |
| Subscription-ID | UUID | Yes | Subscription identifier for which this notification is being sent |
| Sequence- Number | String encoded Integer | Yes | Sequence number of the notification; the first notification shall have a value of 0, this value shall be incremented by 1 (one) for all  subsequent notifications |
| Event-Timestamp | Unix time format | Yes | Time when the event occurred in standard Unix time format |
| Event-Signature | String | Yes | HMAC-SHA256 signature proving the  authenticity of the request and data. See [9.2](#_bookmark74) [Events authentication](#_bookmark74) |

846

847 The format of the payload in a notification request depends on the event type for which the 848 subscription was created. [Table 19](#_bookmark90) defines the format of the payload provided in a notification per 849 "eventType" (as received in the payload of the subscription request from the Origin Cloud) that may 850 be sent by the Target Cloud. A Target Cloud shall populate the notification payload for the event 851 type being signalled in the Event-Type HTTP header as defined in [Table 19.](#_bookmark90) The schema definitions 852 for all payloads are provided in [Annex B.](#_bookmark174)

853 Table 19 – Event type to notification payload content

|  |  |  |
| --- | --- | --- |
| Event-Type header population | Notification payload on establishment of the  subscription | Notification payload per subsequent notification |
| subscription\_cancell ed | Not present | Not applicable |
| devices\_registered | Array of all currently registered Device UUIDs | Array containing Device UUIDs that have been registered since the  previous notification was sent. |
| devices\_unregistered | Empty array (i.e. []) | Array containing Device UUIDs for devices that  have been de-registered since the previous  notification was sent |
| devices\_online | Array of all currently online Device UUIDs | Array containing Device UUIDs that have come |
|  |  | online since the previous notification was sent. |
| devices\_offline | Array of all currently offline Device UUIDs | Array containing Device UUIDs for devices that have gone offline since the previous notification was sent |
| resource\_contentcha nged | Current Resource  Representation of the target Resource | Payload of the changed Resource as received by the Target Cloud |
| resources\_published | Array of Links of all published Resources for the Device UUID in the path | Array of Links of all  Resources published by the Device UUID in the path since the previous notification was sent |
| resources\_unpublish ed | Empty array (i.e. []) | Array of Links of all  Resources unpublished by the Device UUID in the  path since the previous notification was sent |

855  9.4.4 Notification response

856 If the Target Cloud receives a non-success path response to a notification request it shall treat the 857 response as indicative of a request to cancel the subscription, and no further notifications for the 858 Subscription ID that was in the request shall be sent. See clauses [9.8.3,](#_bookmark114) [9.9.3,](#_bookmark120) and [9.10.3](#_bookmark126) for 859 further information.

860  9.5 Subscribe and unsubscribe to devices level event types

861  9.5.1 Summary

862 This request is sent from the Origin Cloud to the Target Cloud. An Origin Cloud may use this API 863 when it wants to receive notifications of events generated due to changes to the set of Devices that 864 are exposed.

865 Event types that may be subscribed to using this API are: devices\_registered,

866 devices\_unregistered, devices\_online and devices\_offline.

867 An Origin Cloud may establish a subscription by sending a POST request to the API Endpoint 868 shown in [Table 20.](#_bookmark94) To remove an existing subscription an Origin Cloud shall send a DELETE 869 request to the API Endpoint as shown in [Table 20.](#_bookmark94)

[Table 20](#_bookmark94) provides a summary of the API.

Table 20 – Subscription to /devices API Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HTTP  Request Type | API Endpoint | Parameters | Response Code | Response Payload |
| POST | /api/v1/devices/subscriptions | Correlation-ID, | 201 | See clause |
|  |  | Accept,  Content-Type |  | [B.1](#_bookmark176) -  /definitions/S ubscribeResp |
|  |  |  |  | onse |
|  |  |  | 400, 401, |  |
|  |  |  | 403 |
| DELETE | /api/v1/devices/subscriptions/{subscriptionId} | Correlation-ID | 202 |  |
|  |  |  | 400, 401,  403, 404 |  |

9.5.2 Request and Response payload

The request payload for the POST shall be as defined in clause 9.4.1.

The "subscriptionId" in the URI for the DELETE case shall be the "subscriptionId" that was returned

in the response to the subscription POST request.

The response payload for the subscription POST request shall contain the Subscription ID in a

"subscriptionId" Property as defined in clause [9.4.2.](#_bookmark85)

There is no required payload for a DELETE unsubscribe response.

9.5.3 Responses

A 201 response shall be sent by the Target Cloud in a success case.

A 202 response shall be sent by the Target Cloud following a DELETE request and indicates that the subscription was marked for cancellation; confirmation of the cancellation of the subscription shall be provided by a subsequent notification with an Event-Type of "subscription\_cancelled".

A non-success path response that is indicative of the type of error shall be returned by a Target Cloud if an error scenario is detected. [Table 21](#_bookmark97) lists possible non-success path responses and possible scenarios that may trigger their generation; an implementation may support additional 887 responses as defined by [IETF RFC 2818.](#_bookmark3)

Table 21 – Devices Event Subscription API non-success path responses

|  |  |
| --- | --- |
| Response Code | Response scenario |
| 400 | May be sent by the Target Cloud if the request was malformed or badly constructed |
| 401 | May be sent by the Target Cloud if the request is unauthorized (e.g. an invalid or missing Bearer Token) |
| 403 | May be sent by the Target Cloud if the requestor is known however the OAuth2.0 Access Token Scope of the request is forbidden |
| 404 | May be sent by the Target Cloud if the subscription was not found or the subscribed to Event-Type is not supported |
| 406 | May be sent by the Target Cloud if the media type in the received Accept header is not supported/acceptable |

889

## 9.6 Подписка и отказ от подписки на события уровня устройства

### 9.6.1 Резюме

Этот запрос отправляется из Origin Cloud в целевое облако. Этот API используется, когда Origin Cloud хочет получать уведомления для определенного устройства в целевом облаке.

Типы событий, на которые можно подписаться с помощью этого API: resources\_published и resources\_unpublished.

Origin Cloud может установить подписку, отправив запрос POST в конечную точку API, показанную в таблице 22. Чтобы удалить существующую подписку, Origin Cloud отправит запрос DELETE в конечную точку API, как показано в таблице 22.

Таблица 22 содержит сводку API.

Таблица 22 - Сводка по подписке на API одного устройства

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HTTP  Request Type | API Endpoint | Parameters | Response Code | Response Payload |
| POST | /api/v1/devices/{deviceid}/subscriptions | Correlation-ID, Accept, Content- Type | 201 | See clause  [B.1](#_bookmark176) -  /definitions/S ubscribeResp onse |
| 400, 401,  403, 404 |  |
| DELETE | /api/v1/devices/{deviceid}/subscriptions/{subscr iptionId} | Correlation-ID | 202 |  |
| 400, 401,  403, 404 |  |

### 9.6.2 Полезные данные запроса и ответа

Полезная нагрузка запроса для POST должна быть такой, как определено в пункте 9.4.1.

«Deviceid» в URI запроса должен быть таким же, как «di» Свойство из «/ oic / d» целевого устройства OCF.

«SubscriptionId» в URI для случая DELETE должен быть «subscriptionId», который был возвращен в ответе на запрос POST подписки.

Полезные данные ответа на запрос POST подписки должны содержать идентификатор подписки в свойстве "subscriptionId", как определено в пункте 9.4.2.

Для ответа об отмене подписки DELETE не требуется никакой полезной нагрузки.

### 9.6.3 Ответы

В случае успеха Целевое Облако отправит ответ 201.

Ответ 202 должен быть отправлен Target Cloud после запроса DELETE и указывает, что подписка была помечена для отмены; подтверждение отмены подписки должно быть предоставлено последующим уведомлением с типом события «subscription\_cancelled».

Неуспешный ответ пути, указывающий на тип ошибки, должен быть возвращен Целевым Облаком, если обнаружен сценарий ошибки. В таблице 23 перечислены возможные неуспешные ответы пути и возможные сценарии, которые могут вызвать их генерацию; реализация может поддерживать дополнительные ответы, как определено в IETF RFC 2818.

Таблица 23 - Неудачные ответы API подписки на события устройства

|  |  |
| --- | --- |
| Response Code | Response scenario |
| 400 | May be sent by the Target Cloud if the request was malformed or badly constructed |
| 401 | May be sent by the Target Cloud if the request is unauthorized (e.g. an invalid or missing Bearer Token) |
| 403 | May be sent by the Target Cloud if the requestor is known however the OAuth2.0 Access Token Scope of the request is forbidden |
| 404 | May be sent by the Target Cloud if the subscription was not found or the subscribed to Event-Type is not supported |
| 406 | May be sent by the Target Cloud if the media type in the received Accept header is not supported/acceptable |

## 9.7 Подписка и отказ от подписки на события уровня ресурса

### 9.7.1 Резюме

Этот запрос отправляется из Origin Cloud в целевое облако. Этот API может использоваться Origin Cloud для получения уведомлений от определенного наблюдаемого ресурса, который существует на определенном устройстве в целевом облаке.

С помощью этого API можно подписаться на следующие события: resource\_contentchanged.

Origin Cloud может установить подписку, отправив запрос POST в конечную точку API, показанную в таблице 15. Чтобы удалить существующую подписку, Origin Cloud отправит запрос DELETE в конечную точку API, как показано в таблице 24.

Таблица 24 содержит сводку API.

Таблица 24 - Подписка на Resource API Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HTTP  Request Type | API Endpoint | Parameters | Response Code | Response Payload |
| POST | /api/v1/devices/{deviceid}/{resourcehref}/su bscriptions | Correlation-ID, Accept,  Content-Type | 201 | See clause  [B.1](#_bookmark176) -  /definitions/S ubscribeResp onse |
|  |  |  | 400, 401,  403, 404 |  |
| DELETE | /api/v1/devices/{deviceid}/{resourcehref}/su | Correlation-ID | 202 |  |
|  | bscriptions/{subscriptionId} |  |
| 400, 401, |  |
|  |  |  | 403, 404 |

### 9.7.2 Полезные данные запроса и ответа

Полезная нагрузка запроса для POST должна быть такой, как определено в пункте 9.4.1.

«Deviceid» в URI в запросе должно быть таким же, как «di» Свойство из / oic / d целевого устройства OCF.

«Resourcehref» в URI должен быть таким же, как «href» параметр ссылки для целевого экземпляра ресурса.

«SubscriptionId» в URI для случая DELETE должен быть «subscriptionId», который был возвращен в ответе на запрос POST подписки.

Полезные данные ответа на запрос POST подписки должны содержать идентификатор подписки в свойстве "subscriptionId", как определено в пункте 9.4.2.

Для ответа об отмене подписки DELETE не требуется никакой полезной нагрузки.

### 9.7.3 Ответы

Целевое облако отправит ответ 201 в случае успеха.

Ответ 202 должен быть отправлен Target Cloud после запроса DELETE и указывает, что подписка была помечена для отмены; подтверждение отмены подписки должно быть предоставлено последующим уведомлением с типом события «subscription\_cancelled».

Неуспешный ответ пути, указывающий на тип ошибки, должен быть возвращен Целевым Облаком, если обнаружен сценарий ошибки. В таблице 25 перечислены возможные неуспешные ответы пути и возможные сценарии, которые могут вызвать их генерацию; реализация может поддерживать дополнительные ответы, как определено в IETF RFC 2818.

Таблица 25 - Неудачные ответы API подписки на события ресурса

|  |  |
| --- | --- |
| Response Code | Response scenario |
| 400 | May be sent by the Target Cloud if the request was malformed or badly constructed |
| 401 | May be sent by the Target Cloud if the request is unauthorized (e.g. an invalid or missing Bearer Token) |
| 403 | May be sent by the Target Cloud if the requestor is known however the OAuth2.0 Access Token Scope of the request is forbidden |
| 404 | May be sent by the Target Cloud if the subscription was not found or the subscribed to Event-Type is not supported |
| 406 | May be sent by the Target Cloud if the media type in the received Accept header is not supported/acceptable |

## 9.8 Уведомление о событиях уровня устройств

### 9.8.1 Резюме

Этот запрос отправляется из Target Cloud в Origin Cloud всякий раз, когда есть начальная подписка на событие или событие, для которого существует подписка, происходит, как определено в пункте 9.4.4.

Таблица 26 содержит сводку API.

Таблица 26 - Сводка по API уведомлений / devices

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HTTP Request Type | API Endpoint | Parameters | Response Code | Response Payload |
| POST | /{eventsUrl} | Correlation-ID, | 200 |  |
|  |  | Content-Type,  Event-Type, | 400, 410 |  |
|  |  | Subscription-ID, |  |
|  |  | Sequence-Number, |  |
|  |  | Event-Signature, |  |
|  |  | Event-Timestamp |  |

### 9.8.2 Полезные данные запроса и ответа

«EventsUrl» в URI должен быть значением свойства «eventsUrl», которое было предоставлено в запросе подписки.

Полезная нагрузка в запросе уведомления зависит от типа события, являющегося предметом запроса уведомления; подробности см. в Таблице 19, а дополнительную информацию - в разделе 9.4.3.

### 9.8.3 Ответы

В случае успеха будет предоставлен ответ 200.

При обнаружении сценария ошибки исходное облако должно возвращать ответ о неудачном пути, указывающий на тип ошибки. В Таблице 27 перечислены возможные неуспешные ответы пути и возможные сценарии, которые могут вызвать их генерацию; реализация может поддерживать дополнительные ответы, как определено в IETF RFC 2818.

Таблица 27 - Отклики пути неуспешного пути уведомления о событии устройства

|  |  |
| --- | --- |
| Response Code | Response scenario |
| 400 | May be sent by the Origin Cloud if the request was malformed or badly constructed |
| 401 | May be sent by the Origin Cloud if the request is unauthorized (e.g. an invalid or missing Bearer Token) |
| 403 | May be sent by the Origin Cloud if the requestor is known however the OAuth2.0 Access Token Scope of the request is forbidden |
| 406 | May be sent by the Origin Cloud if the media type in the received Accept header is not supported/acceptable |
| 410 | May be sent by the Origin Cloud if the subscription identified by the Subscription-ID header is no longer valid |

## 9.9 Уведомление о событиях уровня устройства 973

### 9.9.1 Резюме

Этот запрос отправляется из Target Cloud в Origin Cloud всякий раз, когда есть начальная подписка на событие или событие, для которого существует подписка, происходит, как определено в пункте 9.6. Таблица 28 содержит сводку API.

Таблица 28 - Уведомление о сводке API одного устройства

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HTTP Request Type | API Endpoint | Parameters | Response Code | Response Payload |
| POST | /{eventsUrl} | Correlation-ID, | 200 |  |
|  |  | Content-Type  Event-Type, | 400, 410 |  |
|  |  | Subscription-ID, |  |
|  |  | Sequence-Number, |  |
|  |  | Event-Signature, |  |
|  |  | Event-Timestamp |  |

### 9.9.2 Полезные данные запроса и ответа

«EventsUrl» в URI должен быть значением свойства «eventsUrl», которое было предоставлено в запросе подписки.

Полезная нагрузка в запросе уведомления зависит от типа события, являющегося предметом запроса уведомления; подробности см. в Таблице 19, а дополнительную информацию - в разделе 9.4.3.

### 9.9.3 Ответы

В случае успеха будет предоставлен ответ 200

При обнаружении сценария ошибки исходное облако должно возвращать ответ о неудачном пути, указывающий на тип ошибки. В таблице 29 перечислены возможные неуспешные ответы пути и возможные сценарии, которые могут вызвать их генерацию; реализация может поддерживать дополнительные ответы, как определено в IETF RFC 2818.

Таблица 29 - Неуспешные ответы пути уведомления о событии устройства

|  |  |
| --- | --- |
| Response Code | Response scenario |
| 400 | May be sent by the Origin Cloud if the request was malformed or badly constructed |
| 401 | May be sent by the Origin Cloud if the request is unauthorized (e.g. an invalid or missing Bearer Token) |
| 403 | May be sent by the Origin Cloud if the requestor is known however the OAuth2.0 Access Token Scope of the request is forbidden |
| 406 | May be sent by the Origin Cloud if the media type in the received Accept header is not supported/acceptable |
| 410 | May be sent by the Origin Cloud if the subscription identified by the Subscription-ID header is no longer valid |

## 9.10 Уведомление о событиях уровня ресурсов

### 9.10.1 Резюме

Этот запрос отправляется из Target Cloud в Origin Cloud всякий раз, когда есть начальная подписка на событие или событие, для которого существует подписка, происходит, как определено в пункте 9.7. Таблица 30 содержит сводку API.

Таблица 30 - Уведомление о сводке API ресурсов

### 9.10.2 Полезные данные запроса и ответа

«EventsUrl» в URI должен быть значением свойства «eventsUrl», которое было предоставлено в запросе подписки.

Полезная нагрузка в запросе уведомления зависит от типа события, являющегося предметом запроса уведомления; подробности см. в Таблице 19, а дополнительную информацию - в разделе 9.4.3.

### 9.10.3 Ответы

В случае успеха будет предоставлен ответ 200.

При обнаружении сценария ошибки исходное облако должно возвращать ответ о неудачном пути, указывающий на тип ошибки. В таблице 31 перечислены возможные неуспешные ответы пути и возможные сценарии, которые могут вызвать их генерацию; реализация может поддерживать дополнительные ответы, как определено в IETF RFC 2818.

Таблица 31 - Неуспешные ответы пути уведомления о событии ресурса

|  |  |
| --- | --- |
| Response Code | Response scenario |
| 400 | May be sent by the Origin Cloud if the request was malformed or badly constructed |
| 401 | May be sent by the Origin Cloud if the request is unauthorized (e.g. an invalid or missing Bearer Token) |
| 403 | May be sent by the Origin Cloud if the requestor is known however the OAuth2.0 Access Token Scope of the request is forbidden |
| 406 | May be sent by the Origin Cloud if the media type in the received Accept header is not supported/acceptable |
| 410 | May be sent by the Origin Cloud if the subscription identified by the Subscription-ID header is no longer valid |

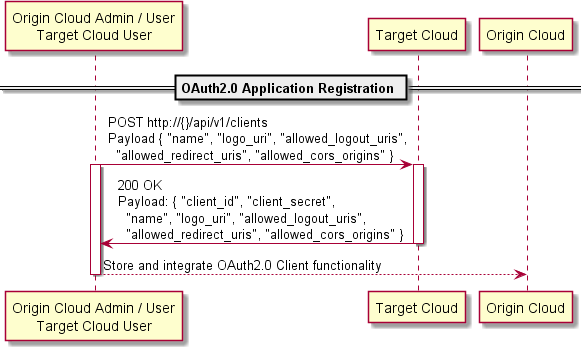
# Annex A Репрезентативные потоки

## А.1 Введение

Потоки иллюстрируют использование OCF Cloud API для облачных служб с использованием устройств OCF в качестве целевых серверов, где это применимо, и облаков OCF в качестве двух облаков, которые вызывают / действуют как конечные точки API. Обратите внимание, что это используется только для примера, и API не требует принудительной настройки, что означает, что облака без OCF с устройствами без OCF также могут использовать API для взаимодействия с облаками других поставщиков.

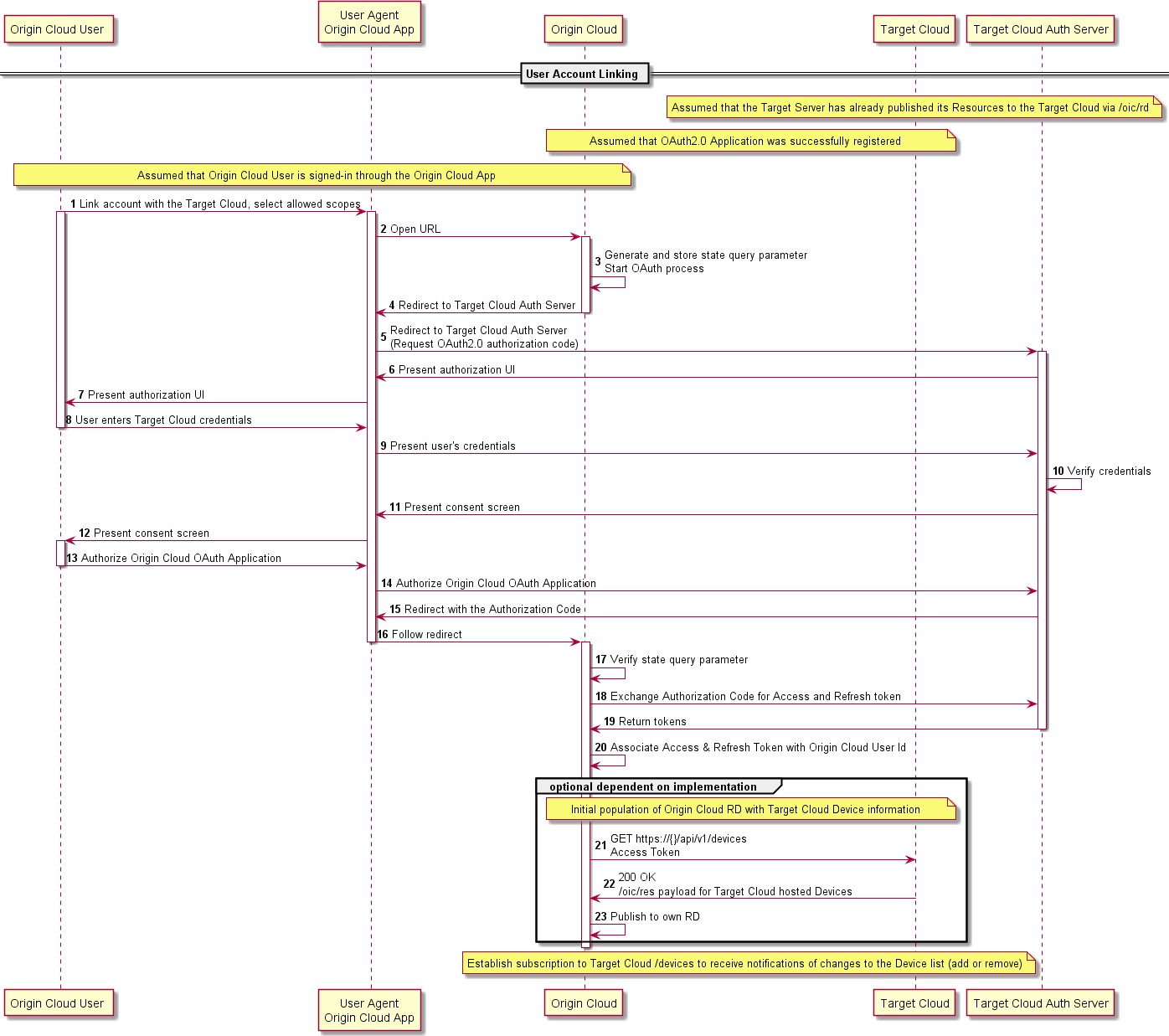
## A.2 Регистрация приложения OAuth2.0

На рисунке A.1 показан пример потока, показывающий регистрацию облачного клиента OAuth 2.0 Origin.

Figure A.1 – Establish business relationship example flow

## A.3 Связывание учетной записи

На рисунке A.2 показан пример процесса привязки учетной записи для конкретного пользователя.

Рисунок A.2 - Пример последовательности операций начальной ассоциации

## A.4 Извлечение всех устройств

### A.4 1 Резюме

Origin Cloud запрашивает все устройства, связанные с пользователем (определяемые предоставленным токеном-носителем). Это может быть вызвано после связывания учетной записи, чтобы получить набор Устройств для пользователя.

### А.4.2 Поток

На рисунке A.3 показан пример потока для извлечения всех устройств..

Figure A.3 – Retrieve all Devices example flow

### А.4.3 Flow description

[Table A.1](#_bookmark139) explains each element in [Figure A.3](#_bookmark137)

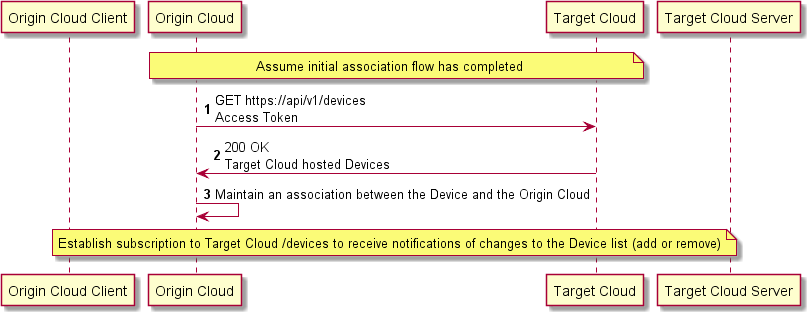


Table A.1 – Retrieve all Devices flow summary

|  |  |
| --- | --- |
| Number | Description |
| 1 | Cloud requests all Devices given by the scope in the Bearer Token that was obtained via OAuth. |
| 2 | Response is an array of Device information ( Properties that are defined in /oic/d that are pertinent to Cloud functionality and Device status). |
| 3 | Cloud maintains an association between the Device and the host Cloud. |

## А.5 Извлечение одного устройства

### А.5.1 Резюме

Origin Cloud запрашивает информацию для одного конкретного Устройства, связанного с пользователем (определяемого предоставленным токеном-носителем). Это может быть вызвано Origin Cloud, получив запрос на извлечение от подключенного Клиента.

### А.5.2 Поток

На рисунке A.4 показан пример потока для извлечения одного устройства..

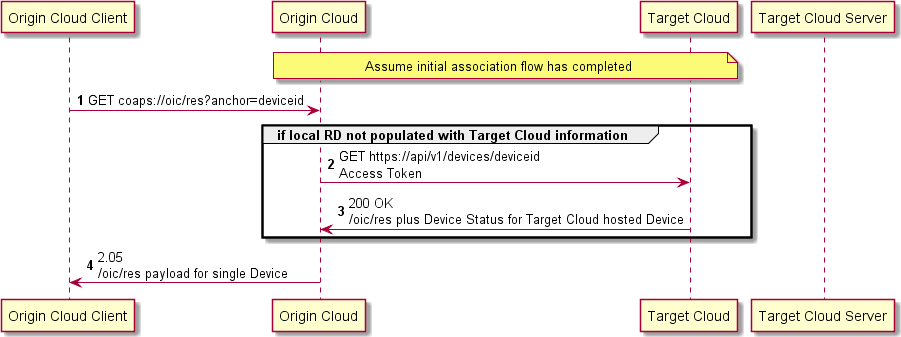


Figure A.4 – Retrieve single Device example flow

A.5.3 Flow description

[Table A.2](#_bookmark145) explains each element in [Figure A.4.](#_bookmark143)

Table A.2 – Retrieve single Device flow summary

|  |  |
| --- | --- |
| Number | Description |
| 1 | [OCF Device to Cloud] OCF Client role Device requests /oic/res from the Cloud for a specific anchor (Device UUID). |
| 2 | [Assuming that the information hasn't been cached by the Cloud]  For the instance of /oic/sec/account that exists for the Device the Cloud does a GET  /devices/{deviceid} to the Cloud identified by the "clouded" in "/oic/sec/account". {deviceid} is also taken from /oic/sec/account. |
| 3 | Response is the Device information as well as an array of Links. The "href" in each Link will be of the form "/deviceid/resourcehref". |
| 4 | Response payload. |

## А.6 Извлечение одного ресурса

### A.6.1 Резюме

Origin Cloud запрашивает информацию об одном конкретном Ресурсе, предоставляемом Устройством, связанным с пользователем (определяемым предоставленным токеном-носителем). Это может быть вызвано Origin Cloud, получив запрос на извлечение от подключенного Клиента.

### А.6.2 Потоки

#### A.6.2.1 Путь к успеху

На рисунке A.5 показан пример потока для получения одного ресурса..

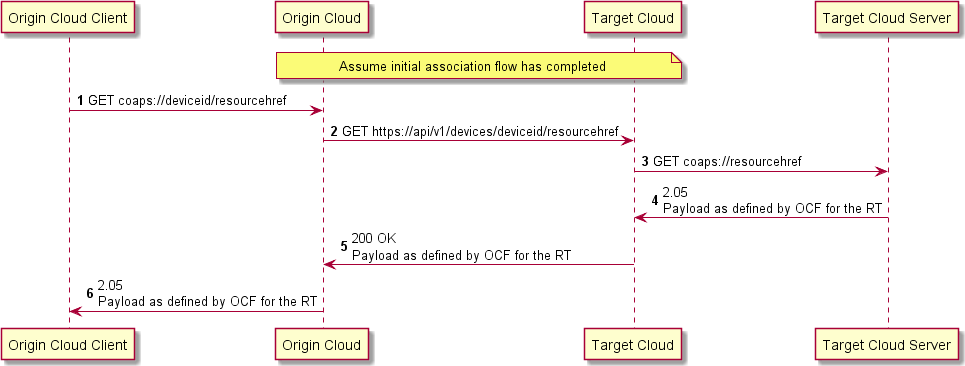


Figure A.5 – Retrieve Resource (success) example flow

#### A.6.2.2 Описание потока пути успеха

[Table A.3](#_bookmark150) explains each element in [Figure A.5.](#_bookmark149)

Table A.3 – Retrieve single Resource flow summary

|  |  |
| --- | --- |
| Number | Description |
| 1 | [OCF Device to Cloud] OCF Client role Device requests a Resource from the Cloud using the "href" exposed in the /oic/res response. This will be of the form "/deviceid/resourcehref" |
| 2 | [Assuming that the resource representation hasn't been cached by the Cloud]  Cloud identifies the host Cloud for the Resource via the instance of /oic/sec/account for the "deviceid". The request is then effectively proxied to the Target Cloud via a GET  /devices/{deviceid}/{resourcehref}. Any query parameters received over CoAP are included in the URI unaltered. |
| 3 | [OCF Device to Cloud] Target Cloud identifies the TLS connection to the end Device via the  {deviceid} and proxies the request. |
| 4 | Standard OCF response |
| 5 | Success path response including the response payload as received for the target Resource |
| 6 | Standard OCF response |

#### A.6.2.3 Устройство временно недоступно

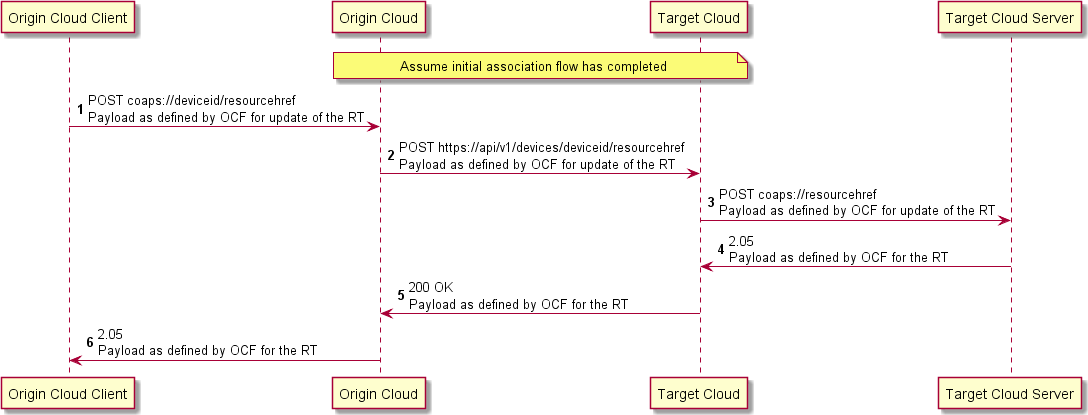
[Figure A.6](#_bookmark151) illustrates the case where the Device is temporarily unavailable.

Figure A.7 – Update Resource (success) example flow

Success path flow description

[Table A.4](#_bookmark156) explains each element in [Figure A.7.](#_bookmark155)

Table A.4 – Update single Resource flow summary

|  |  |
| --- | --- |
| Number | Description |
| 1 | [OCF Device to Cloud] OCF Client role Device requests a Resource from the Cloud using the "href" exposed in the /oic/res response. This will be of the form "/deviceid/resourcehref" |
| 2 | Cloud identifies the host Cloud for the Resource via the instance of /oic/sec/account for the "deviceid". The request is then effectively proxied to the Target Cloud via a POST  /devices/{deviceid}/{resourcehref} including the payload from the original request. Any query parameters received over CoAP are included in the URI unaltered. |
| 3 | [OCF Device to Cloud] Target Cloud identifies the TLS connection to the end Device via the  {deviceid} and proxies the request. |
| 4 | Standard OCF response |
| 5 | Success path response including the response payload as received for the target Resource |
| 6 | Standard OCF response |

Device is temporarily unavailable

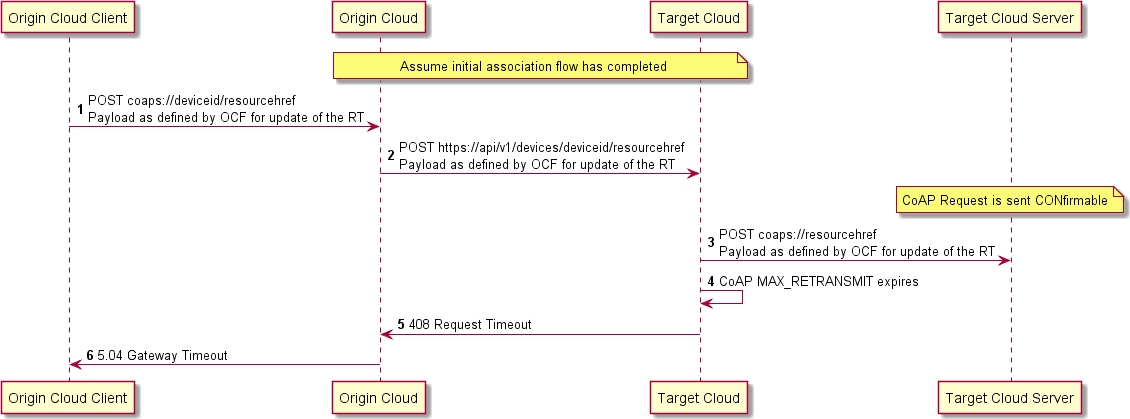
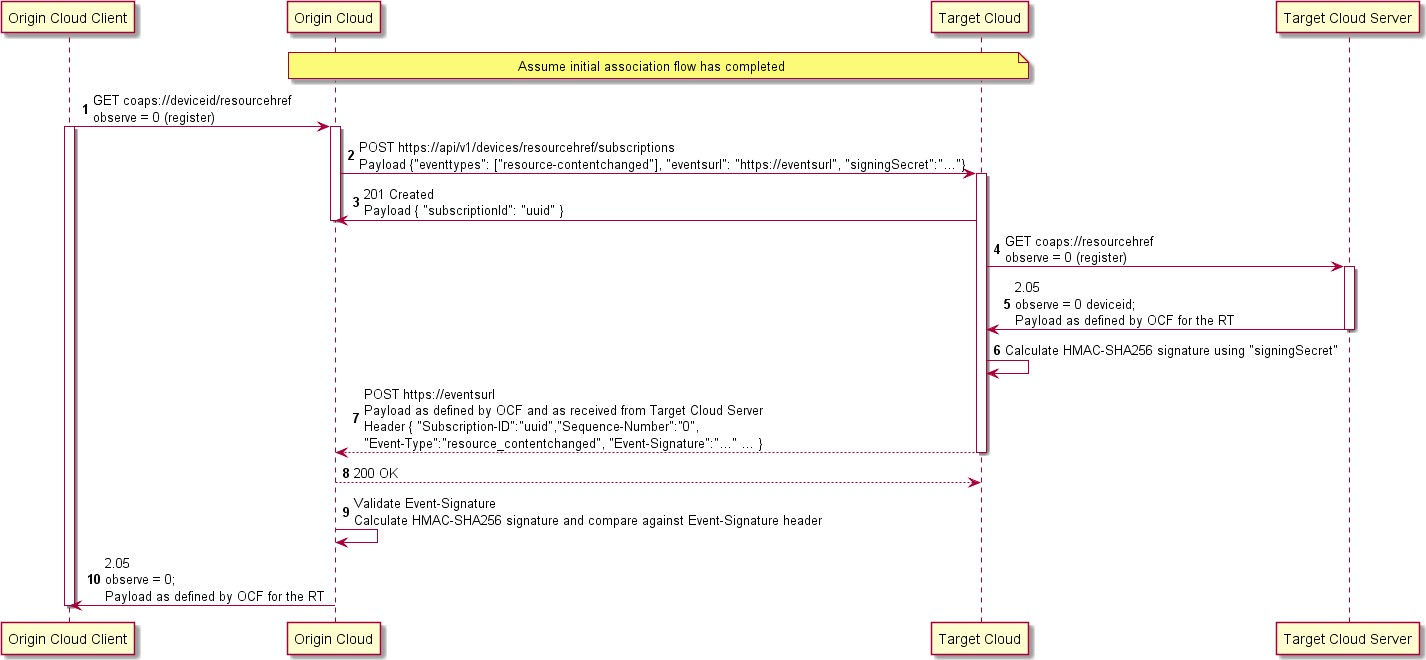
[Figure A.8](#_bookmark157) illustrates the case where the Device is temporarily unavailable.

Figure A.8 – Update Resource (timeout) example flow

A.8 Establishment of new subscription request

A.8.1 Summary

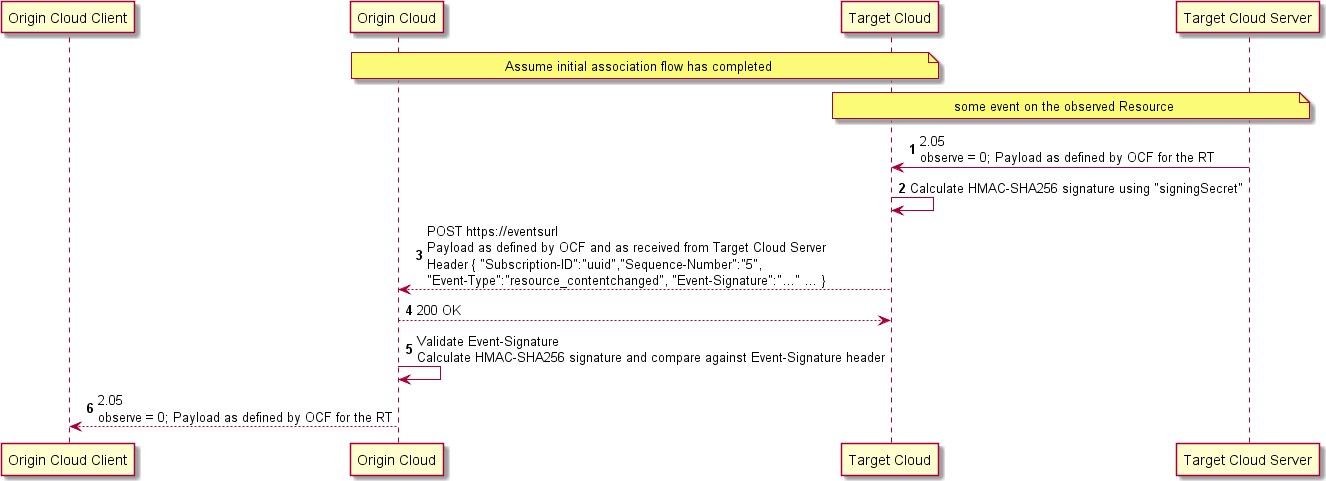
The Origin Cloud requests the establishment of an observe relationship with a single, specific Resource on a Device associated with a user (defined by the provided Bearer Token). This may be invoked by Origin Cloud receiving a retrieve request containing an observe option from a connected Client.

Figure A.9 – Subscription establishment example flow

A.9 Event generated for a subscription

A.9.1 Summary

An event occurs for a Resource with which the Origin Cloud has established a subscription/event relationship. This may be invoked by the target end Device being updated.

A.9.2 Flows

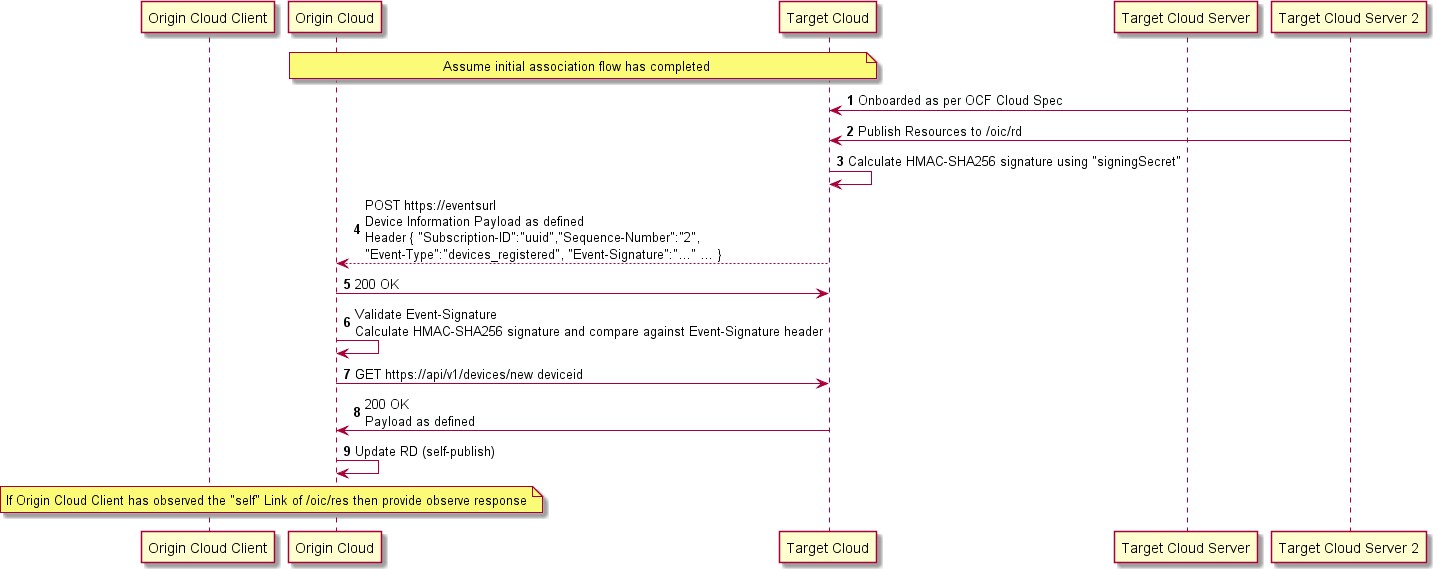
[Figure A.10](#_bookmark165) provides an example flow for the handling of a generated "resource\_contentchanged" event.

Figure A.10 – "resource\_contentchanged" event example flow

A.10 Addition of new registration

A.10.1 Summary

The Origin Cloud has a priori established a subscription/event relationship with the set of Devices associated with a user exposed by Target Cloud. The user then registers a new Device with Target Cloud.



**Figure A.11 – Addition of new registered Device example flow**

**A.11 Removal of existing device registration**

**A.11.1 Summary**

The Origin Cloud has a priori established a subscription/event relationship with the set of Devices

associated with a user exposed by Target Cloud. The user then removes a Device from Target

Cloud.

**A.11.2 Flows**

[Figure A.12](#_bookmark173) provides an example flow for the generation of a notification (event) when a Device is

removed.

A.10.2 Flows

[Figure A.11](#_bookmark172) provides an example flow for the generation of a notification (event) when a new Device is registered.

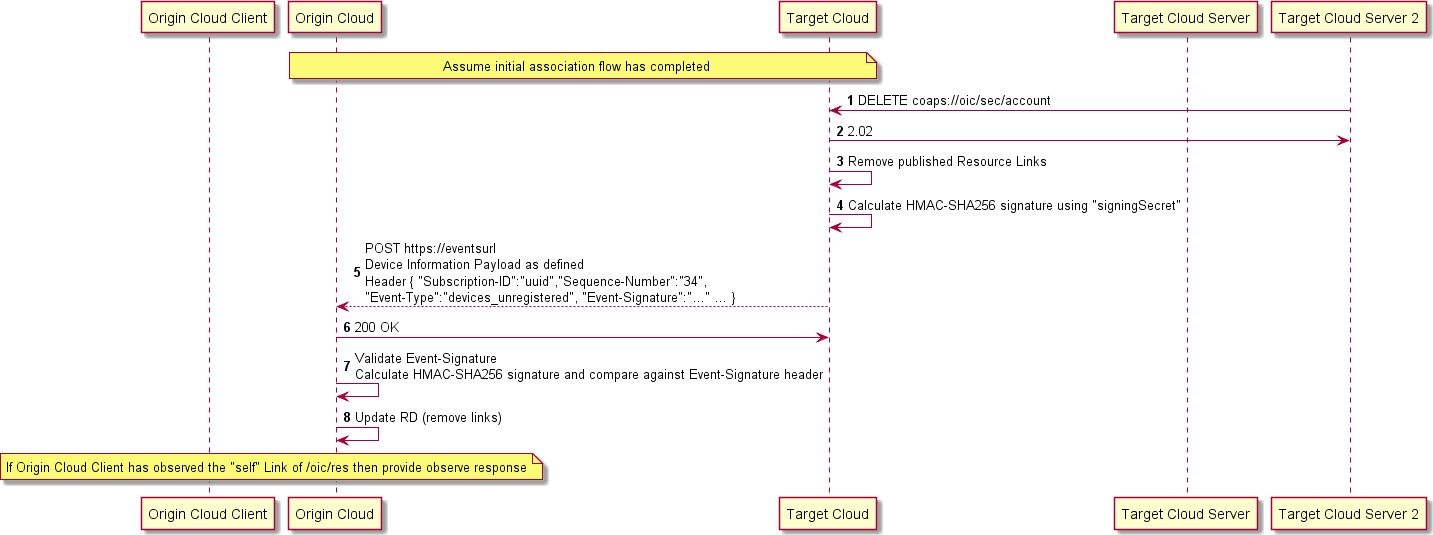


Figure A.12 – Removal of existing registration example flow